NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

UNITED STATES ARMY
LAND MOBILE RADIO COMMUNICATION SYSTEM: IMPACTS OF INFORMATION ASSURANCE ON COMMERCIAL OFF-THE-SHELF SYSTEMS

By: **William D. Chaney,**
Mark Corzine and
Adrianne L. Paolercio

June 2010

Advisors: **Michael W. Boudreau**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE *Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project

4. TITLE AND SUBTITLE:
United States Army Land Mobile Radio Communication System: Impacts of Information Assurance on Commercial Off-the-Shelf Systems

5. FUNDING NUMBERS
N/A

6. AUTHOR(S) : Chaney, William D.; Corzine, Mark; Paolercio, Adrianne L.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES: The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number_________________.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

This Joint Applied Project examined the technical, operational and programmatic implementation of Information Assurance (IA) as it relates to the Commercial-Off-the-Shelf (COTS) Land Mobile Radio (LMR) program within the United States (U.S.) Army. This project provides an overview of the LMR system, its capabilities and technical requirements, as well as the IA processes and requirements. The project then examines the technical aspects and impacts of implementing the IA requirements on the LMR system with possible interoperability with the Global Information Grid (GIG). As a result of this project, the U.S. Army will have a better understanding of the impact of IA on fielded LMR systems and its future impact to critical communications.

14. SUBJECT TERMS
Information Assurance (IA), Commercial Off-The Shelf (COTS), Land Mobile Radio (LMR), DoD Information Assurance Certification and Accreditation Process (DIACAP), Association of Public Safety Communications Officials International (APCO) 25, National Telecommunications and Information Administration (NTIA)

15. NUMBER OF PAGES
71

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

UNITED STATES ARMY LAND MOBILE RADIO COMMUNICATION SYSTEM: IMPACTS OF INFORMATION ASSURANCE ON COMMERCIAL OFF-THE-SHELF SYSTEMS

William D. Chaney
Civilian, United States Army
B.S., Christian Brothers University, 1997

Mark Corzine
Civilian, United States Army
B.S., Bradley University, 1981

Adrianne L. Paolercio
Civilian, United States Army
B.A., Georgian Court University, 1996

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Authors: ____
William D. Chaney

____
Mark Corzine

____
Adrianne L. Paolercio

Approved by: ____
Professor Michael W. Boudreau, Lead Advisor

____
Katrina Willins, Alternate Reader

____
Nathan Smith, Alternate Reader

____
William R. Gates, PhD
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

UNITED STATES ARMY
LAND MOBILE RADIO COMMUNICATION SYSTEM: IMPACTS OF INFORMATION ASSURANCE ON COMMERCIAL OFF-THE-SHELF SYSTEMS

ABSTRACT

This Joint Applied Project examined the technical, operational and programmatic implementation of Information Assurance (IA) as it relates to the Commercial-Off-the-Shelf (COTS) Land Mobile Radio (LMR) program within the United States (U.S.) Army. This project provides an overview of the LMR system, its capabilities and technical requirements, as well as the IA processes and requirements. The project then examines the technical aspects and impacts of implementing the IA requirements on the LMR system with possible interoperability with the Global Information Grid (GIG). As a result of this project, the U.S. Army will have a better understanding of the impact of IA on fielded LMR systems and its future impact to critical communications.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Automated Information System
AM	Amplitude Modulation
AMBE	Advanced Multi-Band Excitation
APCO	Association of Public Safety Communications Officials International
ATO	Authority to Operate
C&A	Certification and Accreditation
C4FM	Constant Envelope 4-Level Frequency Modulation
CAI	Common Air Interface
CDR	Critical Design Review
CL	Confidentiality Level
CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
COA	Course of Action
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
CQPSK	Compatible Differential Offset Quadrature Phase Shift Keying
CRS	Customer Requirements Statement
DA	Department of the Army
DAA	Designated Accrediting Authority
DAG	Defense Acquisition Guidebook
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
CDD	Capability Development Document

CIO	Chief Information Officer
CPD	Capability Production Document
DODD	Department Of Defense Directive
DODI	Department Of Defense Instruction
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FM	Frequency Modulation
FOC	Full Operational Capability
FRP	Full Rate Production
GIG	Global Information Grid
GPS	Global Positioning System
HAIPE	High Assurance Internet Protocol Encryptor
IA	Information Assurance
ICD	Initial Capability Document
IOC	Initial Operational Capability
IOT&E	Initial Operational Test & Evaluation
IP	Internet Protocol
IS	Information System
ISDN	Integrated Services Digital Network
ISSI	Inter-RF Sub-System Interface
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
kHz	Kilohertz
LAN	Local Area Network
LMR	Land Mobile Radio
LRIP	Low Rate Initial Production
MAC	Mission Assurance Category
MAIS	Major Automated Information System

MC/ME	Mission Critical / Mission Essential
MHz	Megahertz
NASTD	National Association of State Telecommunications Directors
NCS	National Communications System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTIA	National Telecommunications and Information Administration
OA	Operational Assessment
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget
P25	Project 25
PC	Personal Computer
POA&M	Plan of Action and Milestones
PM	Project Manager; Program Manager
PSTN	Public Switched Telephone Network
RF	Radio Frequency
SME	Subject Matter Expert
SBU	Sensitive But Unclassified
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TRANSEC	Transmission Security
UHF	Ultra High Frequency
U.S.	United States
VHF	Very High Frequency
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This Joint Applied Project examined the technical, operational and programmatic implementation of Information Assurance (IA) as it relates to the Commercial-Off-the-Shelf (COTS) Land Mobile Radio (LMR) program within the United States (U.S.) Army. This project provides an overview of the LMR system and its capabilities and technical requirements as well as the IA processes and requirements. The project then examines the technical aspects and impacts of implementing the IA requirements on the LMR system, as well as, the drawbacks of integrating LMR onto the Global Information Grid (GIG).

Several Courses of Action (COA) were developed and analyzed to determine possible options that the Project Manager for the LMR program could pursue. These COAs weighed the benefits and consequences of taking no action in implementing IA into the LMR system, integrating the full IA requirements throughout all the architectures and implementing an IA plan for the Platform IT enclave. Following the analysis of the COAs, it was determined that classifying LMR as a Platform IT system would provide the desired security without having significant negative impacts on the funding, operation and performance of the system.

As a result of this project, the U.S. Army will have a better understanding of the impact of IA on fielded LMR systems and its future impact to critical communications.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Land Mobile Radio (LMR) system is the primary means of communication within the first responder community and is critical to the safety and well being of those depending on the reliable operation of the system. LMR systems are fielded as independent United States (U.S.) Army Enterprise sub-systems and leverage unused portions of existing fiber infrastructure at U.S. Army locations to connect LMR system components together in an intranet-style network. In an attempt to increase the capability of the LMR systems, the U.S. Army now plans to incorporate LMR data streams onto the Global Information Grid (GIG). Since the LMR system would now pass voice and data in bit streams, the Department of Defense (DoD) categorized the LMR as an Information Technology (IT) system. According to DoD directives, all IT systems must be compliant and accredited in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP).

LMR systems are Commercial-Off-the-Shelf (COTS) products and are procured and installed in accordance with the prevailing industry standards. In addition to the transmission components of the LMR system, IT networking components, such as servers and routers, have been integrated into the system in order to assist with transporting voice and data through the system. The categorization of the system as an IT system and now the integration of these IT products have forced not only Information Assurance (IA) requirements and processes to be applied to the LMR systems, but has also caused LMR vendors to have to provide "unique solutions" to acceptably meet the DIACAP requirements. Because most of the LMR system components are considered COTS, having to design, develop and implement engineering changes to an already developed and mature product for the new U.S. government specific or unique IA requirements, challenges the idea that these systems are still considered COTS. Since LMR vendors use commercially available products, they are also at the mercy of third party vendors to find adequate resolutions. Current systems offered by vendors are being altered to incorporate these unique design changes due to the stringent IA requirements. This government-unique IA requirement requires COTS modifications and puts a significant cost and technical burden on both the Project Manager (PM) and the user for the future to satisfy the newly levied requirements.

To best determine how significant these impacts are, the primary question that must be answered is, “What is the impact to the LMR system by placing the IA requirements on the COTS components?” Through the following chapters, several supporting questions must also be answered, such as “What are the operational requirements and characteristics of a LMR system?”, “What is the purpose of implementing IA into LMR systems?”, “What are the IA boundaries once the DIACAP is implemented on a LMR system?” and finally, “What are the operational implications of IA on LMR?”, “How does the implementation of IA affect the LMR COTS acquisition concept?” and “Should the DIACAP process be implemented based on these impacts?”

The following chapters, in an attempt to answer the above questions, will provide an overview of the radio, describe the LMR system capability and components as well as provide information on the directives and DIACAP processes and discuss the IA requirements that apply to LMR. Once completed, this paper will assist the DoD and industry in understanding the possible impacts of IA requirements being placed on COTS products and the implication on future LMR implementations.

II. LAND MOBILE RADIO SYSTEM OVERVIEW

A. HISTORY OF THE RADIO

Radio usage and availability began to increase in the early 1900s when the transatlantic telegraph cable was laid across the Atlantic Ocean enabling the first signals to be sent.[1] By the 1930s, one-way broadcasts were available to users such as the police department, followed by a two-way Amplitude Modulation (AM) broadcast capability. Early radio communications used Morse code with dedicated operators. Through the 1940s, Frequency Modulation (FM) capabilities were employed, with the 1950s bringing size and weight reductions that allowed for hand held opportunities to be provided to users. By the 1960s, mobile radios were being delivered for use in public safety radio systems.[2]

As radio technology continued to advance with miniaturization, increased human/machine interfaces and power capability, the two-way radio communications equipment became much more widely used and is now capable of being installed in vehicles. Radio technology continued to advance and mature with large technical working groups focusing on ways to further the abilities of radio communication.[3]

Today's radio equipment, such as the LMR, is designed for ease of use and is widely used by non-tactical personnel for emergency first responder organizations, public works organizations and companies with large fleets of vehicles or numerous field staff. Systems with many individual components are linked together using various technologies to integrate the components and provide ever-increasing coverage for radio users. Just as technology has driven the computer industry to smaller, more powerful personal computers (PCs), the LMR industry has leveraged that technology to provide many more capabilities other than simple voice to the radio user. Today’s users have the ability to scan the Internet, use Global Positioning System (GPS) technology and pass data such as pictures, all through the radio.[4]

The following sections provide background information, as well, as provide an overview of the LMR system, allowing for identification of the operational requirement and the characteristics of the LMR system.

B. LAND MOBILE RADIO BACKGROUND

The Code of Federal Regulations (CFR), Telecommunications section Title 47, defines a Land Mobile Radio system to be, "A regularly interacting group of base, mobile and associated control and fixed relay stations intended to provide land mobile radio communications service over a single area of operation.[5]" The word mobile is used to relate to the motion or movement of a radio system (both hand-held and portable) and not necessarily to a vehicle.[6]

The U.S. Army's LMR system was originally procured to provide a wireless voice communications capability for installation military police, fire departments and medical response units. It provided a local solution to meet site-specific requirements. The U.S. Army LMR systems were non-tactical systems and were not intended to support combat missions or be deployed with a combat force.[7]

The nature of the situation has changed and the U.S. Army LMR system is now an integral part of the Army info-structure. The original requirement has evolved into a requirement to support an installation force protection and public safety network, with a future integrated voice and data transport capability. Particularly since the events of September 11, 2001, the various military installations throughout the country have created interdependencies with the surrounding state and local governments. As a result of the interoperability requirements, the installation LMR network must interconnect with state and local counterpart mobile radio networks. Security concerns have broadened that interdependency from the traditional public safety role to that of an integrated capability to support Homeland Security operations.[8]

C. LAND MOBILE RADIO SYSTEM TECHNOLOGY

Each system's architecture, although individually designed, does have common functional components. LMR system architectures are designed according to a Customer

Requirements Statement (CRS), which identifies a specific user’s needs and requirements. Each customer’s site requirements are different, which means there is not a single architectural solution for all users. An architecture will differ according to the specific components and technologies used.[9]

1. LMR Components

Figure 1 shows the basic components of a LMR system.[10] Each component provides the following function for the overall system:

- Antennas and Repeaters receive and transmit Radio Frequency (RF) signals among radios and with the infrastructure
- Infrastructure provides the backbone of the system and enables connectivity between antennas and control lines
- Control lines connect LMR management facilities to remote sites
- Remote sites serve as a fixed interface to the LMR system, containing consoles, which allow monitoring of multiple end user devices from a central location. They also provide a connection into the system for configuration and management.
- Radios are the end user devices, which transmit and receive the signals from the antennas. Radios can include various form factors such as hand-held, mobile and desktop configurations.

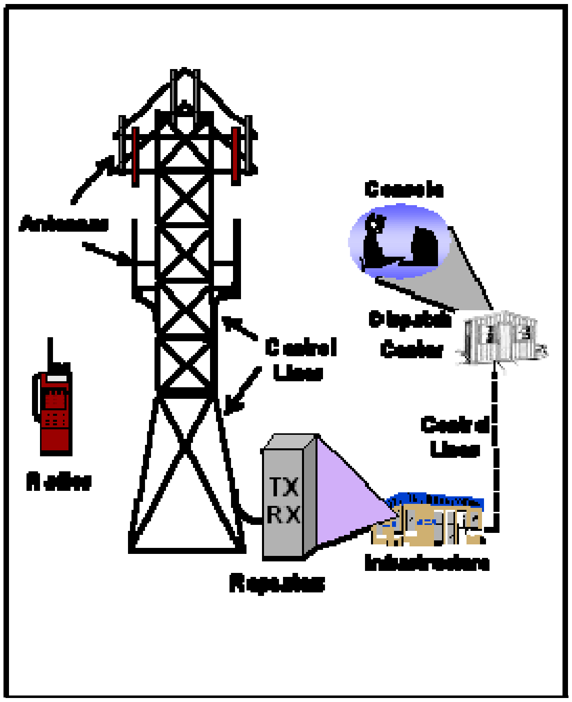


Figure 1. Land Mobile Radio System Components (From: Land Mobile Radio: The Basics, 2008)

The LMR is an integrated system comprised of the components in Figure 1, which work together to provide a near seamless standard of communication. These components can be further grouped by their architectural functions: the subscriber units, the dispatch products and the system infrastructure.

The subscriber unit components consist of the hand-held, mobile and desktop two-way RF communication devices.

The dispatch product components consist of the radio dispatch consoles or dispatch control center and a voice and a data recorder. The system infrastructure consists of several configuration items:

- Comparators: process data collected from multiple receivers to create the best possible transmission signal in multi-cast and simulcast systems
- Subscribers: end-user devices which provide digital communications
- Controllers: provide network access, site database information and an Internet Protocol (IP) interface capability

- System / Network Management Equipment: contain the following:
    - Network Manager: used to view, monitor, and manage the performance of the LMR network
    - Gateway: provides integration capabilities between different LMR systems
    - Switching center: manages the routing and switching of voice messages.

2. LMR Technologies

The technologies utilized in the LMR system address selectable frequency transmission, modulation techniques and channel access to signals. The LMR system is capable of operating in several frequency bands, which are designated for mobile communications by the U.S. National Table of Frequency Allocations. These frequencies usually are in the Very High Frequency (VHF), Ultra High Frequency (UHF) and UHF High Band.[11]

Modulation is the process of encoding information on the transmission side onto a carrier in a manner suitable for transmission with demodulation occurring on the receiving end, which extracts the information from the carrier for processing. The modulation schemes used in the LMR systems are either analog or digital. Analog modulation converts audio voice signals into RF signals in the form of continuous waves. This type of modulation was present in the first generation of the LMR systems. The second modulation technique is digital modulation, which converts the signals into a digital bit stream of ones and zeros. Following a mandate from DoD, LMR systems are to utilize the digital type of modulation in order to achieve the performance advantages of enhanced voice quality, improved spectrum efficiency and reduced background noise and interference.[12]

LMR systems access radio frequencies by using either the conventional or trunking technology, or a combination of both (hybrid). These technologies are detailed in the following paragraphs. The user's unique site requirements dictate which technology is utilized.

Conventional LMR systems work on a simplex mode of operation where only one frequency is used for both transmit and receive. Using fixed RF channels, radios operate on one channel at a time. The proper channel is selected by a user via a channel selector or buttons on the radio control panel to pick the desired channel.

A graphical depiction of this type of approach is shown in Figure 2, as it demonstrates that users are required to stay in one frequency or channel.[13] This conventional approach to communications means that the communication channel is only one-way, so radio users can either transmit or receive, but not simultaneously. Additionally, users are assigned to specific frequencies, which are preprogrammed onto repeaters. This approach can be an inefficient use of spectrum when many radio users need to share the same system. Some repeaters would be at capacity while others would barely have any communication traffic. Conventional technology is simple, has lower costs and is supported by a large number of vendors. The frequencies are dedicated to specific channels, with users having to manually select a voice channel. A negative characteristic to the conventional approach is that when a channel is in use, other users who may want to transmit a signal on that channel must listen and wait for the current users to complete their conversation.

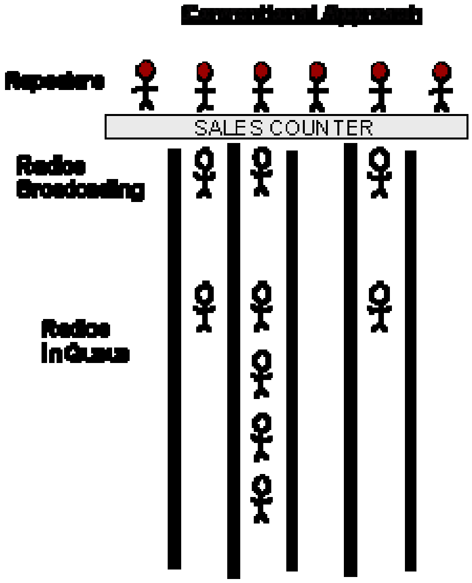


Figure 2. Conventional Approach (From: Land Mobile Radio: The Basics, 2008)

Unlike conventional systems, trunked LMR systems use a full duplex operational mode. Full duplex utilizes two frequencies: one for repeater transmit (radio receive) and one for repeater receive (radio transmit). At any given time, the communications channel is two-way and radio users do not have specific frequency assignments. In a trunked radio system, the system manager automatically selects the physical radio frequency channel. Protocols, which have been developed, help establish the interoperability and compatibility between the radio and the radio backbone or network. These protocols also establish the channel assignments to be selected automatically. One (or more) of the channels is assigned as a dedicated control channel, while the remaining channels are assigned as voice channels. Some of the advantages to using the trunked technology are that it has an increased traffic capacity for a given number of RF channels and during a voice call, the LMR system automatically selects an available voice channel and assigns it to a talk group for increased spectrum efficiency. Figure 3 provides an illustration of a trunked approach.[14]

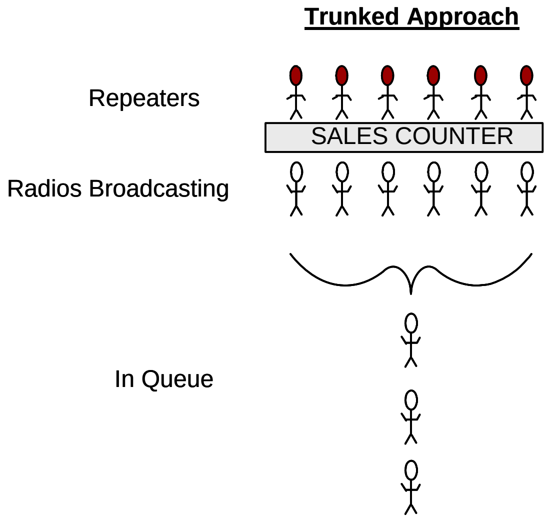


Figure 3. Trunked Approach (From: Land Mobile Radio: The Basics, 2008)

A third configuration is the hybrid system. This system is comprised of a combination of conventional and trunked systems. A hybrid system offers both conventional and trunked features to users within a single system. The advantages and reasons for implementing a hybrid architecture are the cost and call setup delay. When focusing on cost, it may not be cost-effective to have a purely trunked site in an area with just a few users or purely a conventional site where some areas have a higher user density. As stated earlier, every user's requirements and site architectures are different. The second reason is call setup delay. Because it is sometimes important to provide immediate communication in situations, such as for first responders, conventional channels can be implemented to provide dedicated access with minimal call setup delay. The issue comes when other users come on site and are willing to accept the delay and prefer trunked channels to take advantage of the capacity increase. Because no scenario is the same, sometimes a hybrid system architecture is needed to provide conventional and trunked overlays in a single system.[15]

The previous sections described the components and capabilities of the LMR system. The following sections describe the policies and standards the LMR system must follow.

D. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) AND THE NARROWBAND MANDATE

The LMR system falls under the guidance and regulations of the National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce, which is responsible for administering spectrum assigned for federal agency use. The NTIA establishes policies concerning frequency assignment, allocation and use, and also provides the various federal departments and agencies with guidance to ensure that their conduct of telecommunications activities is consistent with these policies. As part of the Executive Branch, the NTIA serves as the President's principle adviser and provides guidance on telecommunications policies involving the economy and technologies as well as helps with the regulation of the telecommunications industry. In addition to these duties, the NTIA presents the position of the Executive Branch to Congress and other agencies such as the Federal Communications Commission (FCC).[16]

In November 1992, the FCC released Docket 92-235 to revise the private Land Mobile Radio services and modify the policies governing them. This was the beginning of the narrowbanding effort, a response to the public safety personnel's request for additional spectrum in the bands below 512 MHz.[17] The decision was made to split the channels from 25 kHz to 12.5 kHz creating additional use of the spectrum. The FCC set forth specific deadlines for systems to meet the narrowbanding mandate. The deadline for federal government users required conversion to narrowband by January 2005 for VHF and January 2008 for UHF.[18]

E. APCO P25 OVERVIEW

An additional group, consisting of several organizations and agencies, joined together to develop a set of standards for radio communications. This effort, named Project 25 (P25), was developed by the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), the National Communications System (NCS) and various Federal Agencies. These policies were standardized by the Telecommunications Industry Association (TIA). The standards were written for digital radio communications primarily used by federal, state and local public safety agencies in North America to enable them to communicate with other agencies and mutual aid response teams in emergencies. The purpose of establishing P25 was to focus on the need for a communications standard for a common digital public safety radio, which would serve to benefit emergency response and Homeland Security personnel.[19]

P25's 'Suite of Standards' specify eight open interfaces between the various components of a land mobile radio system. These interfaces are:

- **Common Air Interface** (CAI) standard specifies the type and content of signals transmitted by compliant radios. A single radio utilizing the CAI should be able to communicate with any other CAI radio, regardless of manufacturer
- **Subscriber Data Peripheral Interface** standard specifies the port through which mobile and portable radios can connect to laptops or data networks

- **Fixed Station Interface** standard specifies a set of mandatory messages supporting digital voice, data, encryption and telephone interconnect necessary for communication between a fixed station and P25 RF subsystem
- **Console Subsystem Interface** standard specifies the basic messaging to interface a console subsystem to a P25 RF subsystem
- **Network Management Interface** standard specifies a single network management scheme, which will allow all network elements of the RF subsystem to be managed
- **Data Network Interface** standard specifies the RF subsystem's connections to computers, data networks or external data sources
- **Telephone Interconnect Interface** standard specifies the interface to Public Switched Telephone Network (PSTN) supporting both analog and Integrated Services Digital Network (ISDN) telephone interfaces
- **Inter-RF Sub-System Interface** (ISSI) standard specifies the interface between RF subsystems which will allow them to be connected into wide area networks

P25-compliant technology, which incorporates these interfaces, is being deployed in several phases. Phase 1 radio systems operate in 12.5 kHz analog, digital or mixed mode and their radios use Constant Envelope 4-Level Frequency Modulation (C4FM) modulation for digital transmissions at 4800 baud and 2 bits per symbol, yielding 9600 bits per second total channel throughput. Radios, which utilize the C4FM standard are also capable of demodulating the Compatible Differential Offset Quadrature Phase Shift Keying (CQPSK) standard since the parameters of the CQPSK signal use the same signal deviation at symbol time as the C4FM and only use 6.25 kHz of bandwidth.

Companies, which have concluded development on the Phase I systems, have ensured that all the requirements in the specifications were followed. These requirements include capabilities such as backwards compatibility and interoperability with other compliant systems. Additionally, the P25 standards require an open standards interface to the RF subsystems, which helps with interfacing to different vendor solutions.

In order to improve spectrum utilization, Phase 2 is currently under development with concurrent work being done on 2-slot Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) modulation schemes. The TDMA and FDMA modulation schemes make up the CQPSK modulation schemes. Phase 2 will use the Advanced Multi-Band Excitation (AMBE) vocoder to reduce the needed bit rate so that one channel will only require 4800 bits per second.

In addition, as part of the Phase 2 work, focus is being placed on interoperability with legacy or older equipment as well as the interfaces between the system components, such as repeaters. Focus is also being given to roaming capacity and spectral efficiency or channel reuse. Phase 2 also looks to help with the human to machine interface to assist operators with training and better operations.

Although interoperability is a key focus of P25, there are still many challenges, especially with interoperability. The P25 systems should theoretically all work together, but since made by different companies, challenges exist with frequencies, training, standard operating procedures and functions. To try to address these challenges and help achieve interoperability, some have scaled back the features and created a “vanilla” P25 implementation. Although this meets the P25 requirements, the intended benefits of P25 are not totally fulfilled.[20]

This chapter has provided an overview of the LMR system, its requirements and characteristics as well as governing bodies who regulate and control the capabilities and performance. The next chapter reviews new directives and organizational users which cause the LMR IA capabilities to be examined.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DIRECTIVE FOR LAND MOBILE RADIO

A. DEPARTMENT OF DEFENSE

In August 2001, DoD issued a policy involving the acquisition of LMR systems. This policy defined Land Mobile Radio and required that all LMR products comply with the security measures set forth in the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 and the DoD Chief Information Officer (CIO) guidance and policy memorandum No. 6-8510 dated 16 June 2000. These two policy requirements set the stage for LMR to, not only be considered an IT product, but to require the need for LMR to be "hardened" in accordance with the DoD GIG IA policies.[21]

This policy, released by the Deputy Secretary of Defense, covered all military LMR assets worldwide, both fixed and mobile. The basic thrust of the policy was to ensure that DoD complied with the upcoming NTIA narrowband mandate in a timely, cost-effective manner. This policy provided definitions for the types of LMR, as well as set the stage for the appropriate levels of encryption and security required.

The policy defined three Information Assurance levels as "levels of robustness" needed to secure LMR based upon its functions. Level one defined a basic level of encryption based on good business practices. Level two, a medium robustness, was determined based on the mission category and/or information sensitivity. At the highest level, level three, was reserved for classified information and mission critical systems.

The policy further defined two types of LMR: tactical and non-tactical. A LMR intended for use in combat, tactical applications or for mission critical applications was deemed tactical LMR and required the highest level of robustness. All other LMRs used for administrative and mission support functions were to be considered non-tactical LMR and would require basic or medium levels of robustness depending on their mission definition.

The DoD policy further directed that all new LMR systems comply with the APCO Project 25 standards.[22] These efforts established a solid foundation from which the state, local and Federal public safety providers could begin to offer mutual aid to one another. Infrastructure and radios that met the Project 25 standards eventually had to communicate in analog mode with legacy analog radios, and systems, and in either digital or analog mode with other Project 25 compliant radios and systems.[23]

B. OFFICE OF HOMELAND SECURITY

After the September 11, 2001 terrorist attacks, it became obvious that LMR, although a vital component to communications during disasters, was woefully inadequate. It became painfully clear that LMR needed to be considered in greater depth and with more planning than initially expected by DoD. Days after the September 11, 2001 terrorist attacks, it was announced by President George W. Bush that the Office of Homeland Security would be created and would have the responsibility to coordinate with other departments and oversee a National Strategy to protect the country.

Later in 2002, the National Strategy for protecting the country was released and identified three objectives:

1. “Prevent terrorist attacks within the United States;
2. Reduce America’s vulnerability to terrorism; and
3. Minimize the damage and recover from attacks that do occur.”[24]

This National Strategy provided direction and guidance for federal departments and agencies on steps to take to improve security. The National Strategy also provided guidance for others such as state and local governments, corporations and businesses and individual citizens.

On November 2002, President George W. Bush signed into law the Homeland Security Act of 2002, which created the United States Department of Homeland Security, resulting in the largest federal government reorganization since the Department of Defense was created via the National Security Act of 1947.[25]

With the creation of this organization, a new group of users would need the LMR system and therefore require greater protection and security measures placed on their communications system.

C. DEPARTMENT OF THE ARMY

In late February 2002, the Department of the Army (DA) issued a memorandum that included an Army Supplement to DoD Land Mobile Radio policy, a Plan for Army LMR Narrowbanding and the Concept for Support to National Homeland Security. LMR was now made an integral part of the Army Infrastructure to support installation Force Protection and Public Safety networks with future integrated voice and data transport capability. The DA made it clear that LMR would be installed to help meet the National Homeland Security mission.[26]

The Concept for Support to National Homeland Security had several objectives. The primary objective was to replace existing LMR infrastructure to comply with the NTIA narrowband mandate while employing commercial standards to maximize interoperability, competition and flexibility. The second objective was to provide the ability for U.S. Army installations to interconnect and communicate with surrounding Federal, State and local Force Protection and Public Safety in an effort to provide incident consequence management. The Concept for Support document also supported the U.S. Army's commitment to contribute to the National mission and assist in the development of capabilities wherever possible.

These acts of policy shaped the current Army Land Mobile Radio program into an IT based system, which requires security commensurate with the information currently being passed through it. After the September 11 attacks, much of the information previously considered sensitive at best, was now considered National Security.

This chapter has provided an overview of the directives and rationale for directing that IA be implemented on the LMR system. The following chapters will provide an overview of the processes and procedures required by DoD for implementing IA into Information Technology systems, such as LMR.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DOD INFORMATION ASSURANCE IMPLEMENTATION

According to the Defense Acquisition Guidebook (DAG), the IT infrastructure for the DoD is called the GIG, a globally connected set of information capabilities. If an IT system is standalone, it is considered Non-GIG IT. The DoD has required that IT system information be protected to ensure availability, integrity, authentication and confidentiality.[27] The directions and instructions to complete this are found in the DoD 8500 series of publications and are required by the PMs to be reviewed for applicability and compliance.[28]

A. DIACAP

In order for DoD Information Systems (IS) to be approved and authorized to operate in their designed environment, they must first undergo a Certification and Accreditation (C&A) process. The C&A process is a set of procedures and assessments meant to verify the suitability of a system to operate.[29] According to the Committee on National Security Systems (CNSS) Instruction Number 4009, certification is defined as, "Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements." Accreditation is defined as, "Formal declaration by a Designated Accrediting Authority (DAA) that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards."[30]

The DoD established this C&A process, known as the DIACAP, found in DoD Instruction (DoDI) 8510.01, to provide guidance and help manage the implementation of Information Assurance capabilities and services or controls. DoD established a policy for all ISs that forms a standard, enterprise process for certifying and accrediting ISs and assists with system compliance with GIG standards as well as the network centric environment. ISs are to follow this process to also help identify and manage risk on their IA capabilities. This process, which replaced the previous method, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), serves as a standard method in which DoD ISs achieve their Authority to Operate (ATO).[31] The main changes made between the DITSCAP and DIACAP are an increased focus on the IA controls to serve as the main security requirements for ISs.[32]

The DIACAP focuses on the C&A process from a lifecycle and enterprise point of view. The DIACAP encourages PMs to have their systems participate in the process early in their system lifecycles. This allows for IA personnel and stakeholders to be involved in the requirements development process. This method benefits the systems by linking the C&A process into the development process, which helps address implementation and system risks. The DIACAP consists of the phases and activities shown in Figure 4.[33]

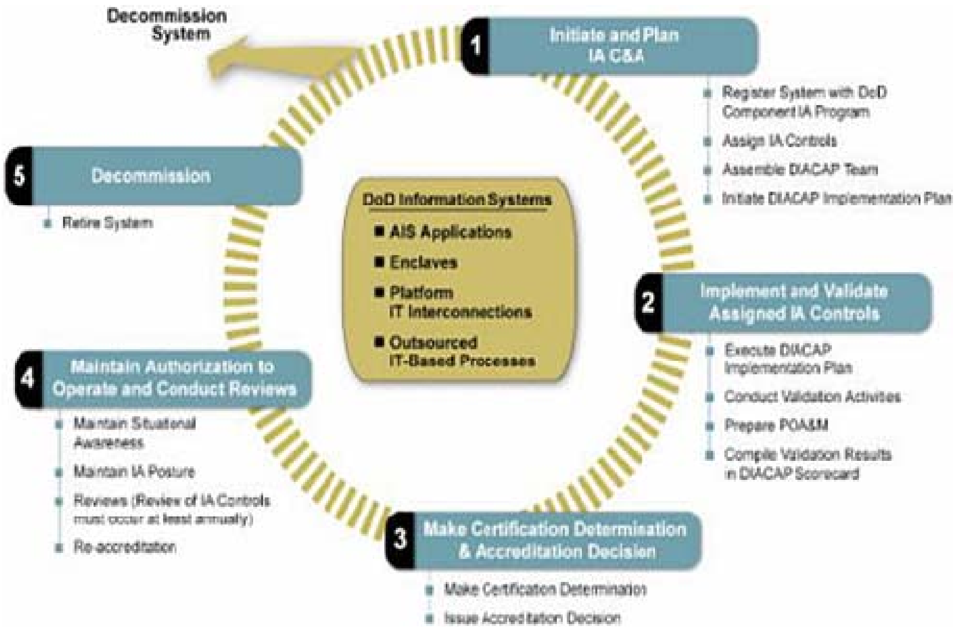

Decommission System
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Prepare POA&M
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness
Maintain IA Posture
Reviews (Review of IA Controls must occur at least annually)
Re-accreditation
5 Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes

Figure 4. DIACAP Activities (From DoDI 8510.01, 2007)

Phase I, Initiate and Plan, focuses on the steps taken by new systems, which involve registering the system with the DoD component and forming a team to develop a plan and work the process. Phase II, Implement and Validate, involves carrying out the system's DIACAP plan and beginning to validate the system. Phase III, Make C&A

Decisions, involves analyzing the risks and determining the C&A path forward. Phase IV, Maintain ATO, involves implementation of the IA controls and maintaining them throughout the life of the system. Periodic reviews are held not less than annually. Phase V, Decommission, is the final phase as the system is reaching its end of life and the processes are closed out.[34]

The typical timeframes associated with this implementation of IA into a program are shown Figure 5. As seen, there are steps taken throughout the lifecycle of the acquisition program.[35]

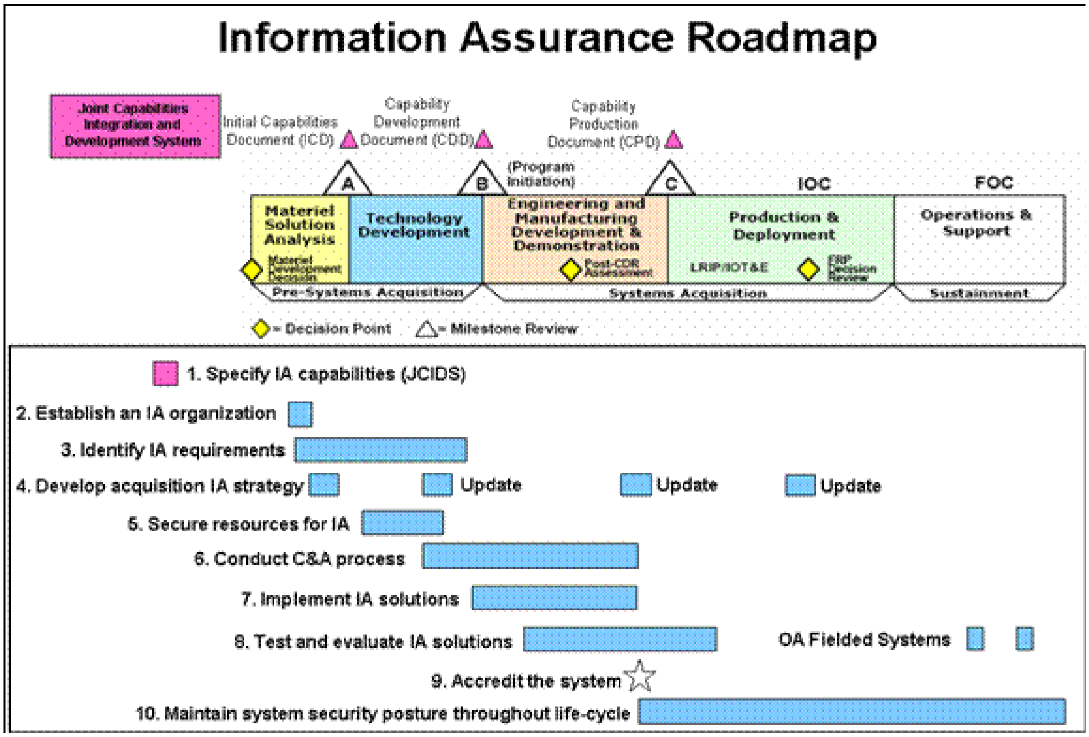

Information Assurance Roadmap
Joint Capabilities Integration and Development System
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
A
B
(Program Initiation)
C
IOC
FOC
Materiel Solution Analysis
Materiel Development Decision
Technology Development
Engineering and Manufacturing Development & Demonstration
Post-CDR Assessment
Production & Deployment
LRIP/IOT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
= Decision Point
= Milestone Review
1. Specify IA capabilities (JCIDS)
2. Establish an IA organization
3. Identify IA requirements
4. Develop acquisition IA strategy
Update
Update
Update
5. Secure resources for IA
6. Conduct C&A process
7. Implement IA solutions
8. Test and evaluate IA solutions
OA Fielded Systems
9. Accredit the system
10. Maintain system security posture throughout life-cycle

Figure 5. Timeframes for IA Activities (From Interim Defense Acquisition Guidebook, 2009)

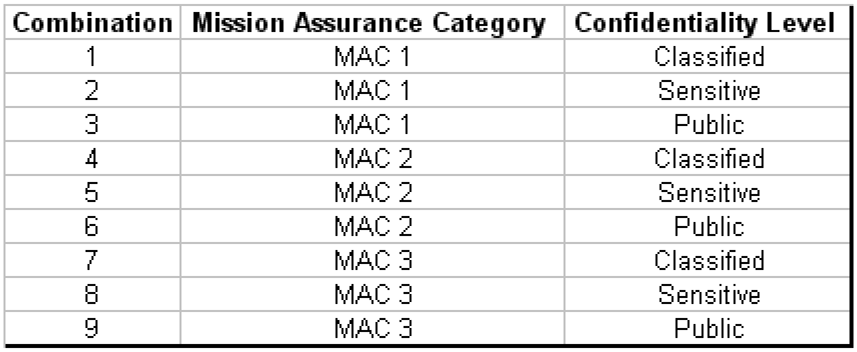
The DIACAP helps ensure ISs receive accreditation and are complaint with the GIG standards by assisting the ISs to implement the IA controls according to DoD directives and legislative policy, such as the IA Department of Defense Directive (DoDD) 8500 series and Federal Information Security Management Act (FISMA). The DoD 8500 series consist of the DoDD 8500.1, DoDI 8500.2, DoDI 8580.1 and DoDI

8520.2 documents and are compliant with the Federal Information Processing Standards (FIPS), which are a set of standards and guidelines issued by the National Institute of Standards and Technology (NIST) for usage in federal computer systems.[36] FISMA, from Title III of the E-Government Act, requires Federal agencies to develop, document and insert a program that will provide IA.[37]

The GIG is a network centric system providing a "globally interconnected, end-to-end set of information capabilities," in order to support the DoD and other agency systems.[38] The GIG is envisioned to provide connectivity and information sharing capabilities to military communities located at all sites to include bases, posts, stations and other facilities and platforms. This network is dependent on the IA components and capabilities in order to provide a defense in depth protection on the information being transmitted. The system's information being transmitted across the network is prioritized and categorized according to the Mission Assurance Category (MAC) and Confidentiality Levels (CL). As required in DoDD 8500.01E, "All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission.[39]"

It is the responsibility of each PM to assign these IA controls, which are assigned based on the MAC and CLs. Both the MAC and CL are defined according to the system requirements or by user representatives and are based upon the system information's importance and criticality to the mission. There are three levels for both the MAC and CLs, with each level representing increasing IA requirements for the information.[40]

Based on its design and its confidentiality level, LMR is categorized as a MAC III sensitive system. Table 1 shows the nine possible combinations of the MAC and CLs.[41]



Combination	Mission Assurance Category	Confidentiality Level
1	MAC 1	Classified
2	MAC 1	Sensitive
3	MAC 1	Public
4	MAC 2	Classified
5	MAC 2	Sensitive
6	MAC 2	Public
7	MAC 3	Classified
8	MAC 3	Sensitive
9	MAC 3	Public

Table 1. Possible Combinations of Mission Assurance Category and Confidentiality Level (After: DoDI 8500.2, 2003)

Since there is countless information being transmitted across many different systems, IA requirements and processes to protect that information must be tailored to fit the mission assurance category and confidentiality levels assigned to that information. As part of the program's lifecycle process, it must be determined what type of system will be developed and what type of information will be transmitted across it. By investigating and reviewing these areas, PMs must determine which IA requirements are applicable. By leveraging guidelines found in DoDD 8500.01E, determination of system type is established and IA requirements applied.

B. DOD INFORMATION SYSTEMS

In general, the term Information System (IS) refers to a system of people, data records or activities that process the data and information in an organization, and it includes the organization's manual and automated processes. In DoDD 8500.01E, an IS is defined as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information. There are several types of IS categorized by: AIS applications, enclaves, outsourced IT-based processes and platform IT interconnections.[42] Each acquisition program containing information technology should fall into one of these categories. IT, defined by DoDI 8500.2, is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component.[43]

Based upon the description above, the LMR system falls into two of the categories for IS, an enclave and the Platform IT. In order to determine the baseline IA requirements for the LMR system, one must look at both the definitions of the enclave and Platform IT, as well as the way in which the system operates to determine the final system type.

An enclave, as defined in DoDD 8500.01E, is a “collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.” The enclave category of DoD IS for LMR can be considered non-GIG IT, since it is a “stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network [44]” Since LMR is a stand-alone information system, it is a subset of the enclave as defined.[45]

Each LMR system architecture is designed and implemented differently, but it is organized or designed based on a specific operating environment and contains an internal network controlled by a single or central management center. Figure 6 shows a notional, LMR system architecture, which has no external interface to an outside system or network.

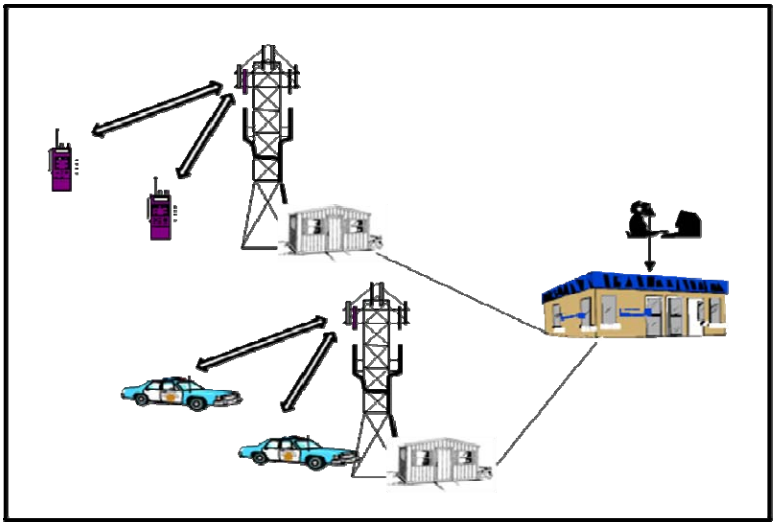


Figure 6. Notional LMR Architecture (After: Land Mobile Radio: The Basics, 2008)

Platform IT, as also defined in DoDD 8500.01E, refers to "computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as … transport vehicles, buildings…[46]" Each Platform IT will have a set of applicable IA requirements when it is stand-alone and a different set of IA requirements when connected to other Platform ITs or to other networks. The connection or the Platform IT interconnection is the, "network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations.[46]" Examples of these Platform IT connections that require IA considerations include communications interfaces for information transmission with enclaves for the purpose of mission planning or execution, remote administration as well as for remote upgrade or reconfiguration tasks. Figure 7 shows an example architecture, with an enclave connected to an external network utilizing an interconnection.

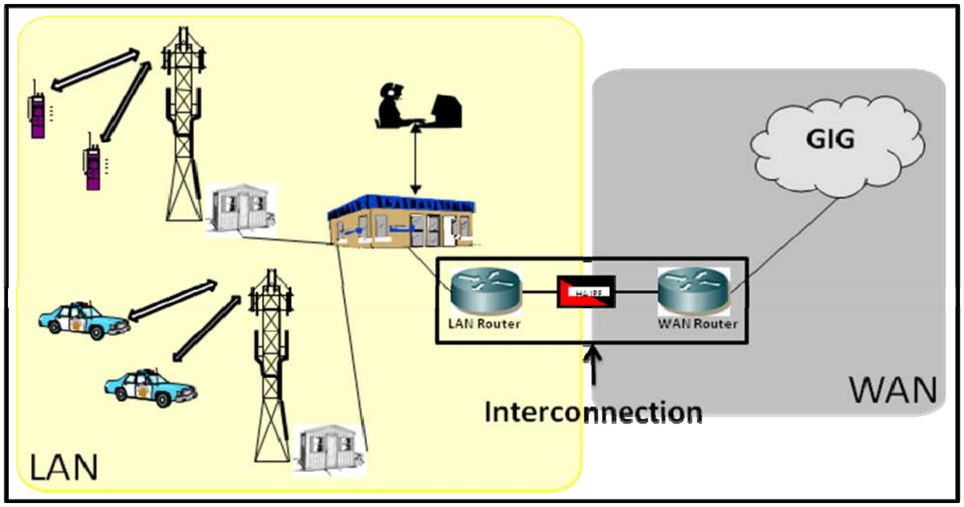
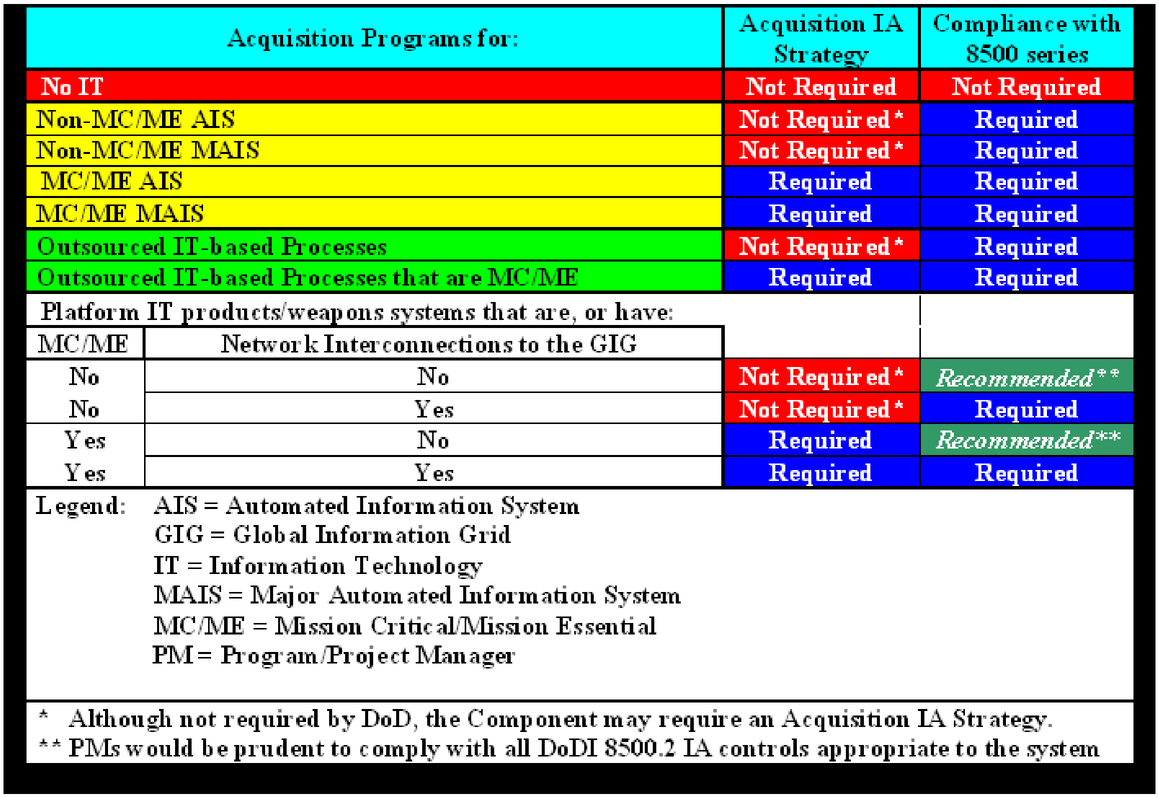


Figure 7. Notional Architecture with Interconnection (After: Land Mobile Radio: The Basics, 2008)

To best determine the applicability and the extent of the IA requirement impact to the LMR system, one must determine exactly which DoD IS category and implementation of LMR architecture should apply and what the boundaries should be. Figure 8 shows how acquisition programs can be categorized and helps determine the IA requirements and policies should be followed.[48]



Acquisition Programs for:		Acquisition IA Strategy	Compliance with 8500 series
No IT		Not Required	Not Required
Non-MC/ME AIS		Not Required*	Required
Non-MC/ME MAIS		Not Required*	Required
MC/ME AIS		Required	Required
MC/ME MAIS		Required	Required
Outsourced IT-based Processes		Not Required*	Required
Outsourced IT-based Processes that are MC/ME		Required	Required
Platform IT products/weapons systems that are, or have:			
MC/ME	Network Interconnections to the GIG		
No	No	Not Required*	*Recommended***
No	Yes	Not Required*	Required
Yes	No	Required	*Recommended***
Yes	Yes	Required	Required

Legend: AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical/Mission Essential
PM = Program/Project Manager

* Although not required by DoD, the Component may require an Acquisition IA Strategy.
** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system

Figure 8. IA Compliance by Acquisition Program Type (From Interim Defense Acquisition Guidebook, 2009)

PMs can attempt to determine which path forward should be followed. LMR is not an Automated IS (AIS) or Major AIS and is not outsourced, so the top portion of the figure would not apply. Based on the information provided above, LMR could be considered a Platform IT. Since the system is relied upon by first responders and Department of Homeland Security (DHS) personnel, it could also be categorized as a mission critical / mission essential system. In looking at the figure, a system IA strategy would be needed and the DoDD 8500 series (DIACAP process) would only be required if LMR is connected to the GIG.

C. DOD IA PROCESS APPLICABILITY FOR LAND MOBILE RADIO

Land Mobile Radio has been defined by DoD as a radio, which operates in a frequency band, designated for mobile communications.[49] The U.S. Army's Land Mobile

Radio Program is considered non-tactical since the radios are used in an administrative capacity for garrison security, emergency response, logistics and maintenance. As a non-tactical form of communication, DoD has further stated that, "Non-tactical LMRs likely to be used for communicating Sensitive But Unclassified (SBU) information shall meet medium or basic robustness…[50]"

The DoDD 8500.01E, paragraph 2.3, identifies the applicability and scope of the directive and states that it (DoDD 8500.01E) "does not apply to weapons systems as defined by DoD Directive 5144.1 or other IT components, both hardware and software, that are physically part of, dedicated to or essential in real time to a platform's mission performance where there is no platform IT interconnection."[51]

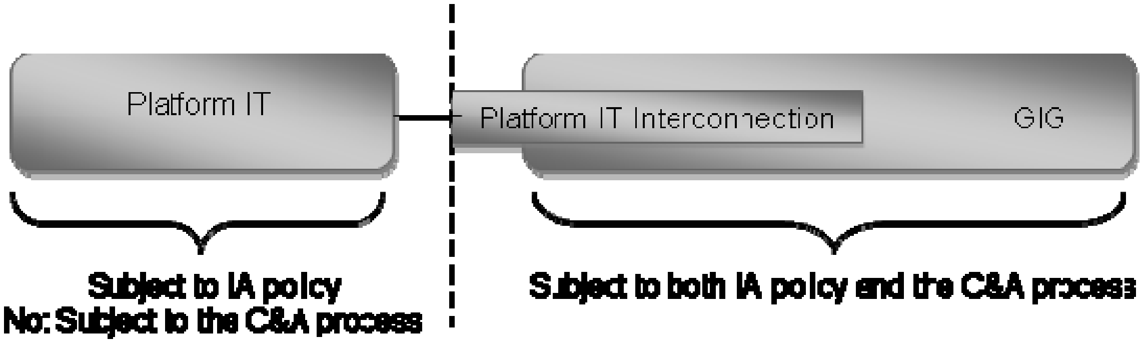

Platform IT
Platform IT Interconnection
GIG
Subject to IA policy
No: Subject to the C&A process
Subject to both IA policy and the C&A process

Figure 9. Platform IT (From DON CIO Memo 01-09, 2009)

As illustrated in Figure 9, generally all GIG related IT is subject to IA policy and the C&A process, but Platform IT is excluded from the C&A process.[52] The Platform IT Interconnection is the only aspect of Platform IT specifically subject to the C&A process, per DoDD 8500.01E and DoDI 8510.01. Furthermore, DoDD 8500.01E states that a stand-alone system, which is a system that does not have any connections to the network, will follow the C&A process, unless it meets the Platform IT categorization. Just because a system is categorized as stand-alone, it is not automatically a Platform IT.

Although there is not an official Determination Statement by the fielding PM, the following apply to Land Mobile Radio as it is currently being fielded. LMR is a stand-alone system used to receive and transmit voice communications within a base operations setting. Its special-purpose mission is essential in real time. It does not provide general IT services, such as e-mail, common office applications, networking for one or more non-Platform IT systems, or business functions.

The IA policy applies generally to all Information Systems. It is the responsibility of the systems' PM to ensure that the IA controls are inserted into the system, even if there is no formal C&A process. PMs should ensure that the maximum IA controls, according to their mission, are inserted into their systems, regardless of whether they are designated as Platform IT. As stated by the DAG, "PMs for acquisitions of Platforms with IT that do not interconnect with the GIG retain the responsibility to incorporate all IA protective measures necessary to support the platform's combat or support mission functions."[53]

Per Defense Acquisition Policy (the DoD 5000 series, and DoDI 8580.1), IA is applicable to all DoD- and Army-owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of MAC or CL.[54]

The Army and Defense Acquisition Policies are satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets. Solutions should be of the appropriate robustness, as determined by the relative strength of the mechanism, and the confidence that the solutions are implemented and perform as intended. The IA solutions that provide availability, integrity and confidentiality also provide authentication and non-repudiation.

The goal of IA for DoD/Army IT systems, as stated in DoDD 8500.1E, paragraph 4.2 is, "All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness.[55]"

The IA Controls provided in DoDI 8500.2 apply to the definition, configuration, operation, interconnection and disposal of DoD information systems. They form a management framework for the allocation, monitoring, and regulation of IA resources that is consistent with Federal guidance provided in Office of Management and Budget (OMB) Circular A-130.[56]

Based upon the above statements from the various DoD Directives and Instructions, the IA requirements for the system are based upon the system status of the LMR system. As stated previously, if operating as a separate system in either a stand-alone system or as a separate Platform IT, the process is greatly different than if the LMR system is to connect to an outside network and utilize an IT Interconnect. The boundaries of the system are architecture dependent. Should the system be stand-alone, then only a tailored DIACAP process would apply. Should the system connect to an external network, then the LMR system must go through the C&A process. Operationally, after a standalone system is fielded, it would be a significant security impact to the system to have it connected to an external network. If this interconnection were to occur, after fielding, the design of the system would have to be modified in order to successfully complete accreditation.

In this chapter, the DIACAP processes and the implications of IA systems were reviewed. Now that it has been established what the applicability of the C&A process and the IA policy for IT systems is, the next chapter will attempt to address the various courses of action that the PM can take to address the IA requirements for the LMR system. The following chapter will examine how the implementation of IA affect the LMR COTS acquisition and to what extent the DIACAP process should be implemented.

V. ANALYSIS OF IA REQUIREMENT APPLICATION OF LMR

A. INTRODUCTION

Developing a clear understanding of the impact that Information Assurance requirements have on existing COTS products is challenging due to the complexity of information systems in general and the ever-changing climate that requires directives and guidance to constantly transform to keep up with security risks. To that end, this chapter analyzes the extent to which the U.S. Army LMR acquisition concept for COTS LMR should or should not be modified to reflect altering existing COTS products to satisfy current DoD initiatives as well as to what extent the C&A (DIACAP) process should be implemented in the LMR system. In order to assess the best course of action, we must first identify what some of the alternatives are.

B. COURSES OF ACTION (COA)

The purpose of this section is to analyze possible alternatives or courses of action (COAs) available for dealing with IA on COTS LMR products. This section addresses three possible courses of action that a PM could pursue when considering how to implement IA on their COTS LMR products system. These are:

1. Take No Action
2. Implement the Full IA Requirements Throughout All Portions of the LMR Architecture
3. Implement an IA Plan for Platform IT with no interconnect to the network

As each course of action is reviewed, the impact that alternative has on funding, resources, time and overall security will also be discussed.

1. COA 1—Take No Action

This COA involves not making any changes to the current LMR system architecture or designs and continuing to follow the current Concept of Operations

(CONOPS). Deciding not to take any action and do nothing could be an alternative for an architecture that consists of COTS products that stand alone and therefore have no security impacts on other systems.

By not altering the LMR architecture or making any design changes to COTS LMR products, this approach allows maximum funding to be allocated to providing the currently designed LMR systems to the Army, leveraging commercial pricing and practices to the greatest extent possible. All Army LMR resources could remain dedicated to the acquisition and integration of these LMR systems into the field and providing the latest technology to first responders. As no changes would be made to the system or the acquisition processes, the time needed to acquire the system and install at desired locations would not change from how operations are done currently. Furthermore, any innovations or updates to the current LMR capabilities created by the vendors could be instituted quickly into new systems without the need for extensive validation and verification. Since in this instance, the LMR system would be a standalone system and not interconnected to any external systems or networks (including the GIG), it can be assumed that the system could operate as it currently does today without any major security or operational impacts. Given that all critical system components are operated and stored in secure areas within an installation, it could also be assumed that physical security would not be an issue. Also, by not changing the current system, there would also be no impacts to the logistics or training requirements.

Some of the concerns that exist concerning this COA are that this would be in violation of the directives given by the DA. As a result, there could be cuts in funding and resources, placing the PM’s program in jeopardy of being cut. The system would operate as it currently does, but not be as secure as leadership would like. The system could become vulnerable as technology advances are made by adversaries to impede the performance and capability of the LMR system. Another downside to the “take no action” option is that the LMR system would have to remain an isolated system and a method for providing information produced on external systems to the first responders would need to be developed. Operationally, the users would suffer as sensitive information would have to be transmitted over alternative systems, resulting in two networks needed to provide information. If it ever came to that and it was decided that changes should be made after all, then any changes made to implement IA requirements would require extra time and significant efforts to modify the LMR system.

2. COA 2—Implement the Full IA Requirements Throughout All Portions of the LMR

This approach employs the tenets of defense-in-depth for layering IA solutions within and among IT assets. The IA solutions have the appropriate robustness, as determined by the relative strength of the mechanism by which they are employed and the confidence that the solutions are implemented and perform as intended. The IA solutions that provide availability, integrity and confidentiality also provide authentication and non-repudiation for the LMR system. This approach presumes that the LMR system would be protected as if it were on, or connected to the GIG.

This COA would provide the most robust security features and therefore the most operationally secure solution. The security measures that would be instituted would provide an appearance of a much more secure system (than with COA approach 1 or 3) designed to keep out such concerns as computer bugs, viruses and worms, in addition to other adversarial "hack" into the LMR system. The IA security measures would account for physical, operational and most importantly, cyber security.

Although the LMR system would have an appearance of greater security, pursuing this approach would require a significant increase in funding and resources to incorporate the IA control measures required. This approach would put a burden on the funding available for all LMR systems. Additional funding would have to be requested, and if enough funding was not provided capabilities would be sacrificed to pay for the increased IA requirements. Additional resources would be required to accommodate the full IA effort, to include the LMR architecture to protect it from interfaces to external systems and the GIG. Additional man-hours would be required not just initially, but throughout lifetime of the system. Vendors would be forced to change their commercial LMR system designs to comply with new IA requirements. Furthermore, vendors would have to make changes to their established support and design processes, and in some cases, create all new divisions in their organizations dedicated to implementing these new IA security requirements. In the PM office, Subject Matter Experts (SMEs) would be required to assist the PM with the ATO process and provide guidance on writing the new IA requirements. Experts proficient in IA regulations would be required to draft and coordinate the necessary paperwork to get final ATO approvals to operate the LMR system. These SMEs would be required by the PM to not only assist the government, but also the vendors as they proceed through the acquisition and DIACAP process. All of these actions would require increased funding and would negatively impact the LMR production schedules such that required capabilities would delay fieldings.

Implementing the aforementioned comprehensive C&A process and following the DIACAP fully would require identifying baseline configurations, authenticating all vendor hardware and software, as well as approving all systems before being allowed to operate. These are just the LMR specific areas that would need to be evaluated during DIACAP. The "presumed" interfaces and interoperability between the LMR and external systems and networks, such as the GIG, would also need to be fully analyzed and new designs for these interfaces developed. Additional time would definitely be required should this option be chosen. Many of the IA requirements identified by the government would only be able to be performed by the Original Equipment Manufacturers (OEM) directly. This would require additional time for third party products to "catch up" to IA requirements that have been levied on them by the LMR prime vendors. Additional system scans, validations, checks, as well as time for coordination throughout the government would be required and additional time to the LMR schedules.

This full-scale C&A process would test and validate all vendors' hardware and software, as well as third party hardware and software that would be used in the vendors' LMR systems. Vendors would be required to modify their LMR system designs to comply with the approved list of products identified by the National Information Assurance Partnership (NIAP).[57] In addition, other security measures for background checks for vendors and fences around areas containing LMR hardware would need to be evaluated.

After the initial approval process was completed and the ATO provided, ongoing LMR system scans and updates would have to be provided by the vendor to keep up with any new security threats. Seeing as a new ATO is required every three years, these processes and efforts to update security in the LMR would be ongoing. As time progresses, LMR system hardware technology would change and many of the hardware components that currently comprising the system would need to be replaced or updated only due to "security" threats, to keep up with IA policy revisions. This would require the vendor to upgrade the system with new components that meet the new IA requirements and that these components work with the existing ones in the LMR system and are backwards compatible.

In addition, personnel in the PM office would be required to be trained on this new process and how it affects their LMR customers. The customers in the field would also be required to undergo training to learn the new IA capabilities of the new hardware and software. As new equipment would be added to the system architecture, the logistics trail would be affected as well.

3. COA 3—Implement an IA Plan for Platform IT with No Interconnect to the Network

This approach pursues a solution in between those proposed in the previous two COAs. LMR is a stand-alone, self-contained radio platform that can be categorized as non-GIG IT and can therefore be considered, based on its mission, a Platform IT system. As such, it would be subject to IA policies but not the full-blown DIACAP C&A process. This COA proposes that IA be integrated onto the Platform IT or "enclaved" LMR system, with no interconnection to external systems, such as the GIG.

The Platform IT approach would require minimal IA implementation and support since the system would be separate and not at risk from attacks originating from external systems. Seeing as the LMR is Platform IT, the need for accreditations to operate every three years or have constant maintenance to upgrade the IT equipment would be unnecessary. This would greatly reduce the funding burden that a full blown C&A effort has on a system, creating cost avoidance. Additionally, manpower to design and accommodate the IA effort is minimal in comparison to COA 2 above. This would allow for the IA Subject Matter Experts (SMEs) to only be required during the production phase of the LMR system. No funding or resources would be required to design and develop an interconnection to various external systems or networks, thus easing the funding burden on the PM. The time required to designate a LMR system as Platform IT and implement an IA program to support it would be minimal in comparison to COA 2 above. The oversight and the number of organizations involved with interconnecting to the GIG would be eliminated, thus reducing time for coordination and other activities. The PM would retain the responsibility to incorporate IA and the controls that would be implemented. The time necessary would be solely based on the system and the direction given by the PM. The security and IA capabilities of the Platform IT could be increased by simply incorporating or enhancing the COMSEC and TRANSEC capabilities. By not having an interconnection (to outside networks or to the GIG), the LMR system would still be able to operate securely, but without the increased network related IA controls that do not add to the IA controls of the "stand-alone" LMR. By not significantly impacting the current system's architecture, the system would be able to maintain its level of readiness and availability. The amount of overhead on the system's links resulting from the additional "network" IA policies being implemented on the LMR would be absent. Congestion and blockages would not be as significant, as the system would not have an increased amount of users from the external systems. Without the extra equipment needed to interface with the external networks, the training duration and difficulty would be lessened. The operators would only be responsible for the Platform IT equipment, without the distraction from external system equipment. Logistically, the trail would be shorter with fewer transport mechanisms needed to get equipment to the field, whether for initial fielding or replacements. By reducing the amount of systems and equipment needed to focus on, the maintenance and personnel support could be reduced as well.

Although there are positive aspects to this COA, there are several negative areas to consider also. Even though, the costs would be less expensive than COA 2, which involved the interconnection, the funding required to implement this COA would still be an increase to the current program’s funding line. Additional resources would still be needed for this COA, as new equipment would be needed to provide the IA enhancements as well as a team of personnel to get involved to ensure the new IA requirements could be implemented without incurring a significant negative impact on the mission and operation of the system. The time needed to implement these changes could have a negative impact on milestones and decision points already scheduled at that time. The system would need to be fully tested to determine if any capabilities would be lost as a result of implementing the IA features, as well as determine if there would be any performance degradation. Since there would be additional equipment and security features implemented, there would be an increase in the logistics tail as well as an increase in maintenance support. The users of the system would also have to be trained on the new features and operation of the system. The logistics considerations would be new to the PM and therefore be an increased drain on resources.

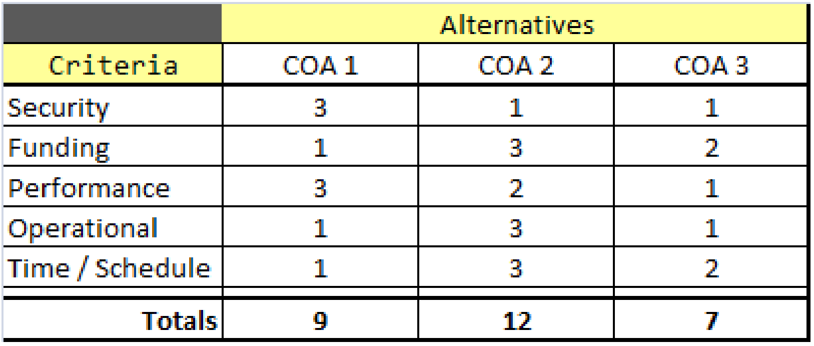
THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

In the previous chapter, three possible courses of actions for dealing with IA on COTS products were identified and analyzed. Through the analysis of these COAs, several factors were identified that could be used as decision aids in determining which COA would be most beneficial to the U.S. Army. In reviewing the three COAs discussed, only one alternative provides minimal impact to the U.S. Army while increasing the security integrity of the system. In determining the optimal COA, a decision matrix was developed to assess the value of each of the five factors.

The criteria selected for the decision matrix were as follows: funding and resources, time, security, performance of the system following the changes and operational impacts. Each of these factors was identified and discussed in the analysis section. The order of importance, determined based on current mission requirements and policies, is: 1) IA Security. The sole purpose of these changes is to make the system more secure from an IA point of view. 2) Funding. Affordability is a priority due to increasing funding shortfalls. 3) Performance. The system has a mission to operate continuously and cannot be impacted by security measures. 4) Operational or logistical impacts. The logistics and maintenance impacts should not be significant. 5) Time. Schedule impacts to the system as a result of implementing security can not jeopardize mission implementation.

Table 2, which follows, shows the matrix used to assist in making the decision. It identifies the criteria and the rating for each COA. The criteria were ordered on the chart according to importance. The ratings assigned to each COA were determined based on how well that COA met the criteria. These were rated on a scale of 1 to 3, with 1 being the best. The COA with the lowest total score would be identified as the best COA to pursue.



	Alternatives		
Criteria	COA 1	COA 2	COA 3
Security	3	1	1
Funding	1	3	2
Performance	3	2	1
Operational	1	3	1
Time / Schedule	1	3	2
Totals	**9**	**12**	**7**

Table 2. COA Decision Matrix (From: Chaney, Corzine, Paolercio, Authors, 2009)

As shown, it was determined that COA 3 is the most favorable and should be pursued.

COA 1, the “take no action” option, is always available to those willing to accept the consequences. However, in the current posture of Information Technology and the ever-growing need to protect information as part of our “War on Terror,” this option is not really an acceptable alternative for a PM. Although this option was scored the second best, it should not be considered. This COA scored best in the funding, time and operational criteria only due to the fact that no changes would be made to the current system and therefore there would be no impacts in these areas. It scored the worst in the most important factor, security, and as a result, shows that it could not meet the requirements to implement IA into the LMR system.

COA 2, implementing the full C&A requirements, is a costly, time-consuming process that may be overkill. The likelihood that a significant amount of LMR communications would be added to the GIG is relatively small. Although incorporation of LMR onto the GIG could provide benefits in the future, the IA technology needed to allow the LMR system access is still immature at best. Furthermore, LMR communications must have top-priority status on any architecture to be effective. Their nature as a life-saving First Responder system puts LMR in grave danger when added to such a massive, high usage network, such as the GIG. This is evident by having the worst score. Although, the security would be the most robust, the other factors suffer greatly.

COA 3, Implement an IA Plan for Platform IT Enclave, is the recommendation of this team. The third COA, Platform IT, should be considered the only option. In addition to the savings in time, funding and manpower resources, Platform IT would alleviate the need to re-certify the system every three years. Historically, LMR systems have a lifespan of 10–15 years without the need to upgrade or replace major hardware. With the insertion the C&A process, many of these systems would require major hardware and software upgrades to maintain security of the GIG, long before the LMR life cycle is expended. This could ultimately cost the government billions of dollars in unnecessary upgrades to equipment that is, essentially, in acceptable working condition.

THIS PAGE INTENTIONALLY LEFT BLANK

END NOTES

[1] Transatlantic telegraph cable (Wikipedia, 2009)

[2] Short History of Radio: With an Inside Focus on Mobile Radio (FCC.gov, 2009)

[3] Two-Way Radio (Wikipedia, 2009)

[4] Land Mobile Radio: The Basics (APM LMR, 2008)

[5] Title 47-Telecommunications (U.S. GPO, 2008)

[6] Mobile Radio (Answers.com, 2009)

[7] Concept of Operations for Implementing Land Mobile Radio Systems (U.S. Army, 2006)

[8] Homeland Security Act of 2002 (U.S. GPO, 2002)

[9] Land Mobile Radio: The Basics (APM LMR, 2008)

[10] Land Mobile Radio: The Basics (APM LMR, 2008)

[11] Land Mobile Radio: The Basics (APM LMR, 2008)

[12] Army Plan for Narrowband Systems Operating in the LMR Service (Secretary of the Army, 2002)

[13] Land Mobile Radio: The Basics (APM LMR, 2008)

[14] Land Mobile Radio: The Basics (APM LMR, 2008)

[15] Comparisons of Conventional and Trunked Systems (SAFECOM, 1999)

[16] Elizabeth C. Borja, Brief Documentary History of the Department of Homeland Security: 2001-2008 (DHS History Office, 2008)

[17] Kathy J. Imel, James W. Hart, and others, Understanding Wireless Communications in Public Safety. (National Institute of Justice, 2003)

[18] Policy for Land Mobile Radio (LMR) System (Deputy SECDEF, 2001)

[19] Pete Lunness Ali Mehrpouyan, Steve Burfoot, Peter Chan, and Dale Reitsma, P25 Radio Systems Training Guide (Daniels Electronics Ltd., 2007)

[20] Project 25 Technology Interest Group (2009)

[21] Policy for Land Mobile Radio (LMR) System (Deputy SECDEF, 2001)

[22] Policy for Land Mobile Radio (LMR) System (Deputy SECDEF, 2001)

[23] Policy for Land Mobile Radio (LMR) System (Deputy SECDEF, 2001)

24 Elizabeth C. Borja, Brief Documentary History of the Department of Homeland Security: 2001-2008 (DHS History Office, 2008)

25 Homeland Security Act of 2002 (U.S. GPO, 2002)

26 Army Plan for Narrowband Systems Operating in the LMR Service (Secretary of the Army, 2002)

27 Department of Defense Directive, 2007, DoDD 8500.01E

28 Chapter 7: Acquiring Information Technology and National Security Systems, (Interim Defense Acquisition Guidebook, 2009)

29 Applying the DOD Information Assurance C&A Process (DIACAP) – Overview (Hatha Systems, 2006)

30 National Information Assurance (IA) Glossary (Committee on National Security Systems (CNSS), 2006)

31 Department of Defense Instruction, 2007, DoDI 8510.01

32 Defense Information Assurance Certifications and Accreditation Process (DIACAP) (GovITwiki, 2009)

33 Department of Defense Instruction, 2007, DoDI 8510.01

34 Mike Bendel, An Introduction to Department of Defense IA Certification and Accreditation Process (DIACAP) (2006)

35 Chapter 7: Acquiring Information Technology and national Security Systems, (Interim Defense Acquisition Guidebook, 2009)

36 Ask a Professor – Question and Answer Detail Communication/Computer System Acquisition (DAU.mil, 2009)

37 Applying the DOD Information Assurance C&A Process (DIACAP) – Overview (Hatha Systems, 2006)

38 Global Information Grid (NSA.gov, 2009)

39 Department of Defense Directive, 2007, DoDD 8500.01E

40 Department of Defense Instruction, 2003, DoDI 8500.2

41 Department of Defense Instruction, 2004, DoDI 8500.2

42 Department of Defense Directive, 2007, DoDD 8500.01E

43 Department of Defense Instruction, 2003, DoDI 8500.2

44 Department of Defense Instruction, 2003, DoDI 8500.2

45 Department of Defense Directive, 2007, DoDD 8500.01E

46 Department of Defense Directive, 2007, DoDD 8500.01E

47 Department of Defense Directive, 2007, DoDD 8500.01E

48 Chapter 7: Acquiring Information Technology and national Security Systems, (Interim Defense Acquisition Guidebook, 2009)

49 Policy for Land Mobile Radio (LMR) System (Deputy SECDEF, 2001)

50 Army Plan for Narrowband Systems Operating in the LMR Service (Secretary of the Army, 2002)

51 Department of Defense Directive, 2007, DoDD 8500.01E

52 Department of the Navy Memorandum, 2009, DON CIO Memo 01-09

53 Chapter 7: Acquiring Information Technology and national Security Systems, (Interim Defense Acquisition Guidebook, 2009)

54 Department of Defense Instruction, 2007, DoDI 8510.01

55 Department of Defense Directive, 2007, DoDD 8500.01E

56 Department of Defense Instruction, 2003, DoDI 8500.2

57 Department of Defense Instruction, 2003, DoDI 8500.2

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Applying the DOD Information Assurance C&A Process (DIACAP) – Overview. Hatha Systems. [Power Point Slides]. 2006.

Army Memorandum, Office of the Secretary of the Army/SAIS-IOM, Subject: "Army Plan for Narrowband Systems Operating in the Land Mobile Radio (LMR) Service," February 26, 2002.

Ask a Professor – Question and Answer Detail Communication/Computer System Acquisition (2009). Retrieved September 2009, from https://akss.dau.mil/askaprof-akss/qdetail2.aspx?cgiQuestionID=21492&cgiSubjectAreaID=3

Bendel, Mike. (2006). An Introduction to Department of Defense IA Certification and Accreditation Process (DIACAP).

Borja, Elizabeth C. (2008). Brief Documentary History of the Department of Homeland Security: 2001-2008. Department of Homeland Security History Office.

Committee on National Security Systems (CNSS). (2006). National Information Assurance (IA) Glossary, CNSS Instruction No. 4009.

Defense Information Assurance Certifications and Accreditation Process (DIACAP) (2009). Retrieved September 2009, from http://govitwiki.com/wiki/Defense_Information_Assurance_Certifications_and_Accreditation_Process_(DIACAP)

Department of Defense Directive (2007). Information Assurance (IA), DoDD 8500.01E.

Department of Defense Instruction (2007). DoD Information Assurance Certification and Accreditation Process (DIACAP), DODI 8510.01.

Department of Defense Instruction (2003). Information Assurance (IA) Implementation, DODI 8500.2.

Department of Defense Instruction. (2004). Information Assurance (IA) in the Defense Acquisition System, DODI 8580.1.

Department of Defense Memorandum, Deputy Secretary of Defense, Subject: "Policy for Land Mobile Radio (LMR) System," August 1, 2001.

Department of the Navy Memorandum, Chief Information Officer, Subject: "Department of the Navy Chief Information Officer Memorandum 01-09, Information Assurance Policy for Platform Information Technology," January 30, 2009

Global Information Grid (2009). Retrieved July 2009, from http://www.nsa.gov/ia/programs/global_industry_grid/index.shtml

Imel, Kathy J., James W. Hart, and others. (2003) Understanding Wireless Communications in Public Safety. National Institute of Justice. Retrieved March 2009, from http://www.npstc.org/documents/GuideWC/Part3(VerII).PDF

Interim Defense Acquisition Guidebook (2009). Chapter 7: Acquiring Information Technology and National Security Systems. Retrieved September 2009, from https://acc.dau.mil/dagch7

Land Mobile Radio: The Basics. Assistant Project Manager, Land Mobile Radio Briefing [Power Point Slides]. U.S. Army Project Manager Defense Communications and Army Transmission Systems (PM DCATS), December 2008.

Lunness, Pete, Ali Mehrpouyan, Steve Burfoot, Peter Chan, and Dale Reitsma. (2007). P25 Radio Systems Training Guide. Daniels Electronics Ltd. Retrieved July 2009, from http://www.danelec.com/library/english/p25_training_guide.asp

Mobile radio: Definition from Answers.com. *Answers.Com*. Answers Corporation, Web. July 2009. Retrieved March 2009, from http://www.answers.com/topic/mobile-radio

National Telecommunications and Information Administration. (2009) Retrieved September 2009, from http://www.ntia.doc.gov

Project 25 Technology Interest Group. (2009). Retrieved August 2009, from http://www.project25.org

SAFECOM. (1999). Comparisons of Conventional and Trunked Systems. Retrieved March 2009, from http://www.safecomprogram.gov/SAFECOM/library/technology/1179_conventionaland.htm

A Short History of Radio: With an Inside Focus on Mobile Radio. Winter 2003–2004: 1-4. Web. January 2009. Retrieved March 2009, from http://www.fcc.gov/omd/history/radio/documents/short_history.pdf

Transatlantic telegraph cable. Wikipedia, the Free Encyclopedia. November 2009. Wikimedia Foundation, Inc., Web. January 2009. Retrieved March 2009, from <http://en.wikipedia.org/wiki/Transatlantic_telegraph_cable>.

Two-way radio. Wikipedia, the free encyclopedia. September 2009. Wikimedia Foundation, Inc., Web. January 2009. Retrieved March 2009, from http://en.wikipedia.org/wiki/Two-way_radio

United States Department of the Army. (2006). Concept of Operations for Implementing Land Mobile Radio Systems.

United States Government Printing Office. (2008) Code of Federal Regulations Title 47 - Telecommunications. Retrieved October 2009, from http://edocket.access.gpo.gov/cfr_2008/octqtr/47cfr90.7.htm

United States Government Printing Office. (2002) The Homeland Security Act of 2002 (Public Law 107-296). Retrieved October 2009, from http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California